Environment-Aware Security

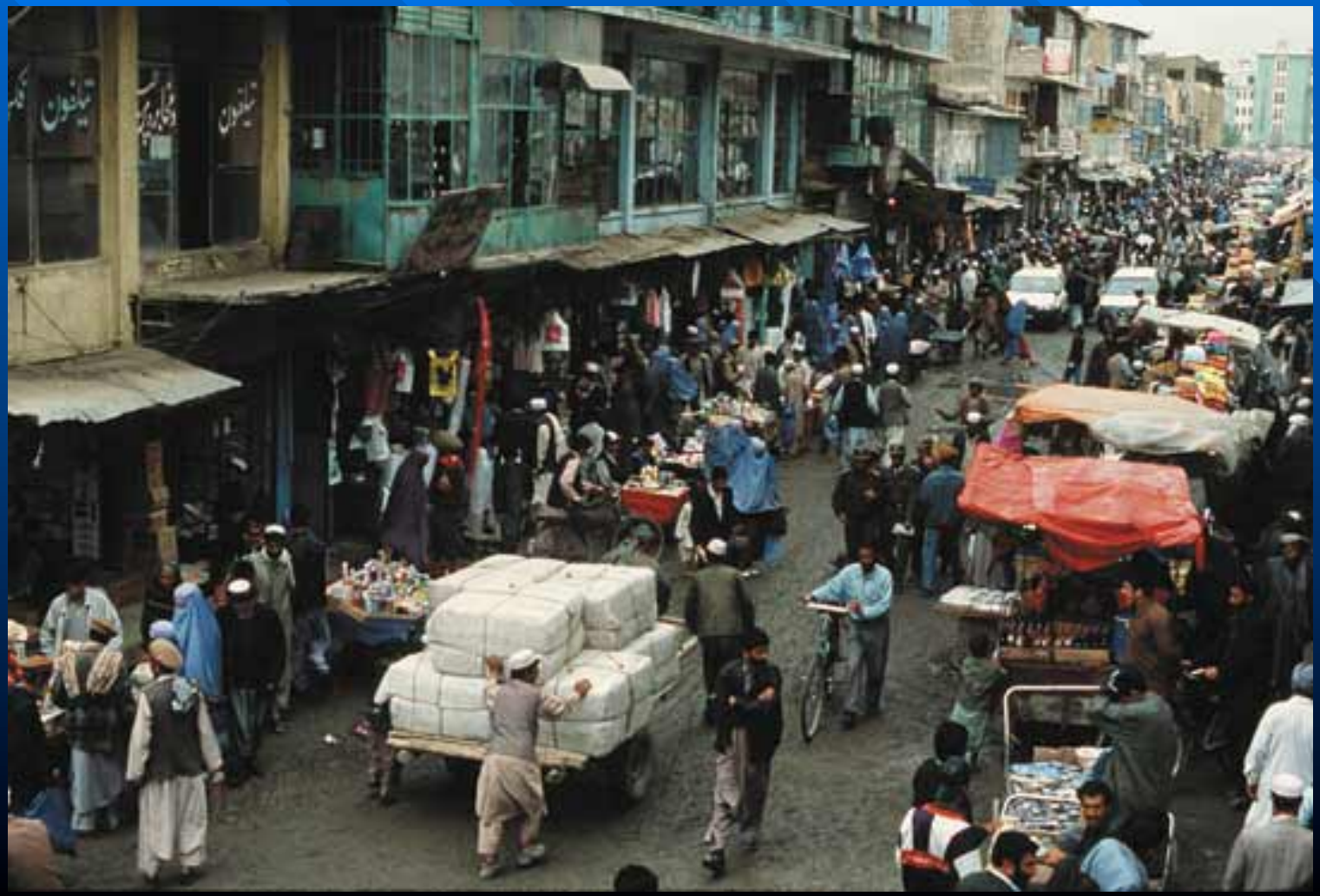
Todd Heberlein
lth@NetSQ.com

Outline

- Ivory Towers, Real Worlds, and Simple Solutions
- Adversaries
- Scale-Free Networks and Power-Law Distributions
- TrendCenter
- Next steps: firewalls and servers
- Going deeper: modeling the enterprise

Ivory Tower of Academia and Research

Real World of Operational Networks



Guiding Principles

If you know the enemy and know yourself, you need not fear the result of a hundred battles.

Sun Tzu

The general who wins a battle makes many calculations in his temple before the battle is fought

Sun Tzu

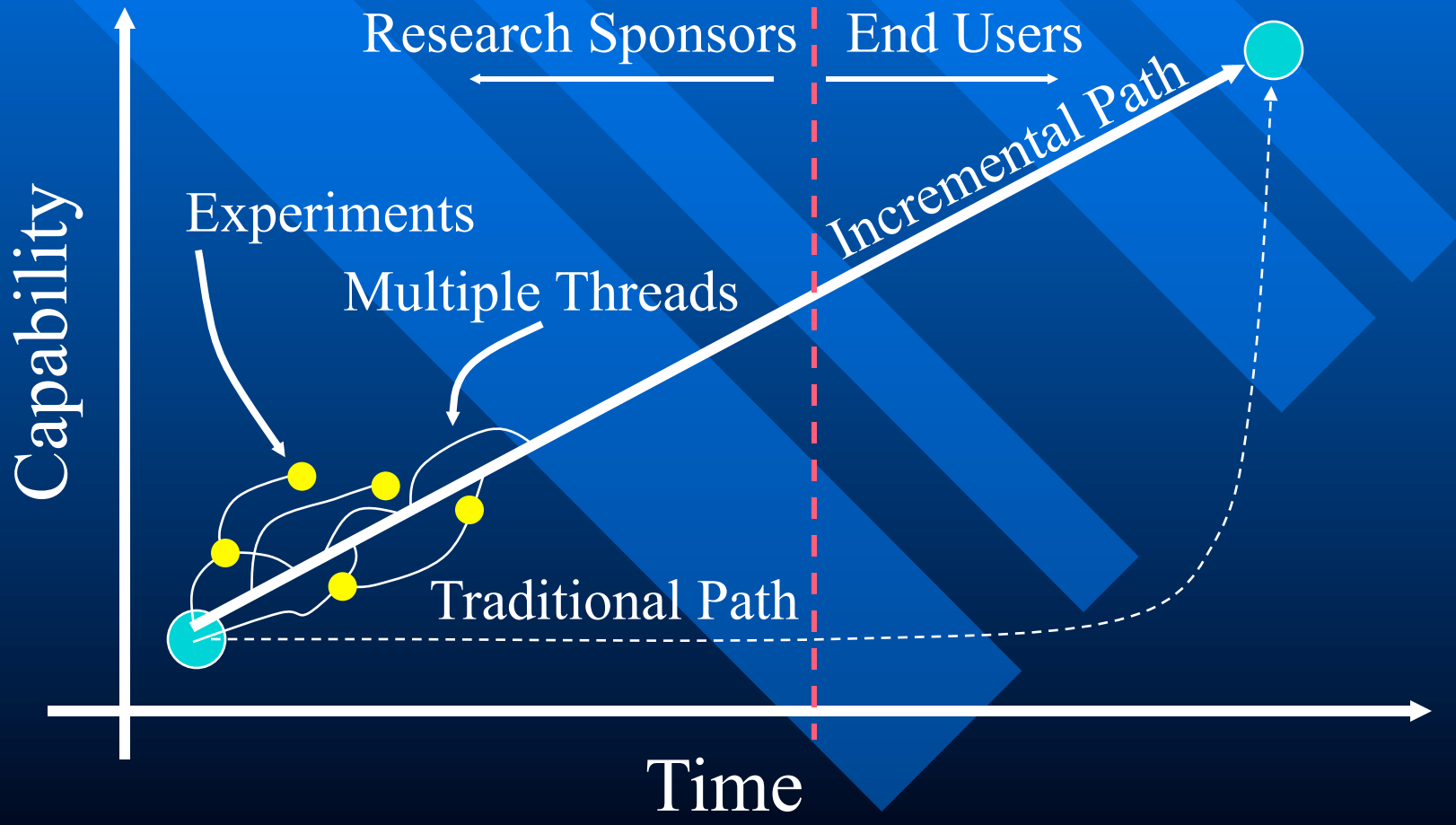
Security is a process, not a product.

Bruce Schneier

When IDS Was Born

- Attacks were extremely rare
- Small number of vulnerabilities known
- Few important systems on the Internet
- System interactions were simpler
- Internet was small and exclusive

eXtreme Research (XR)



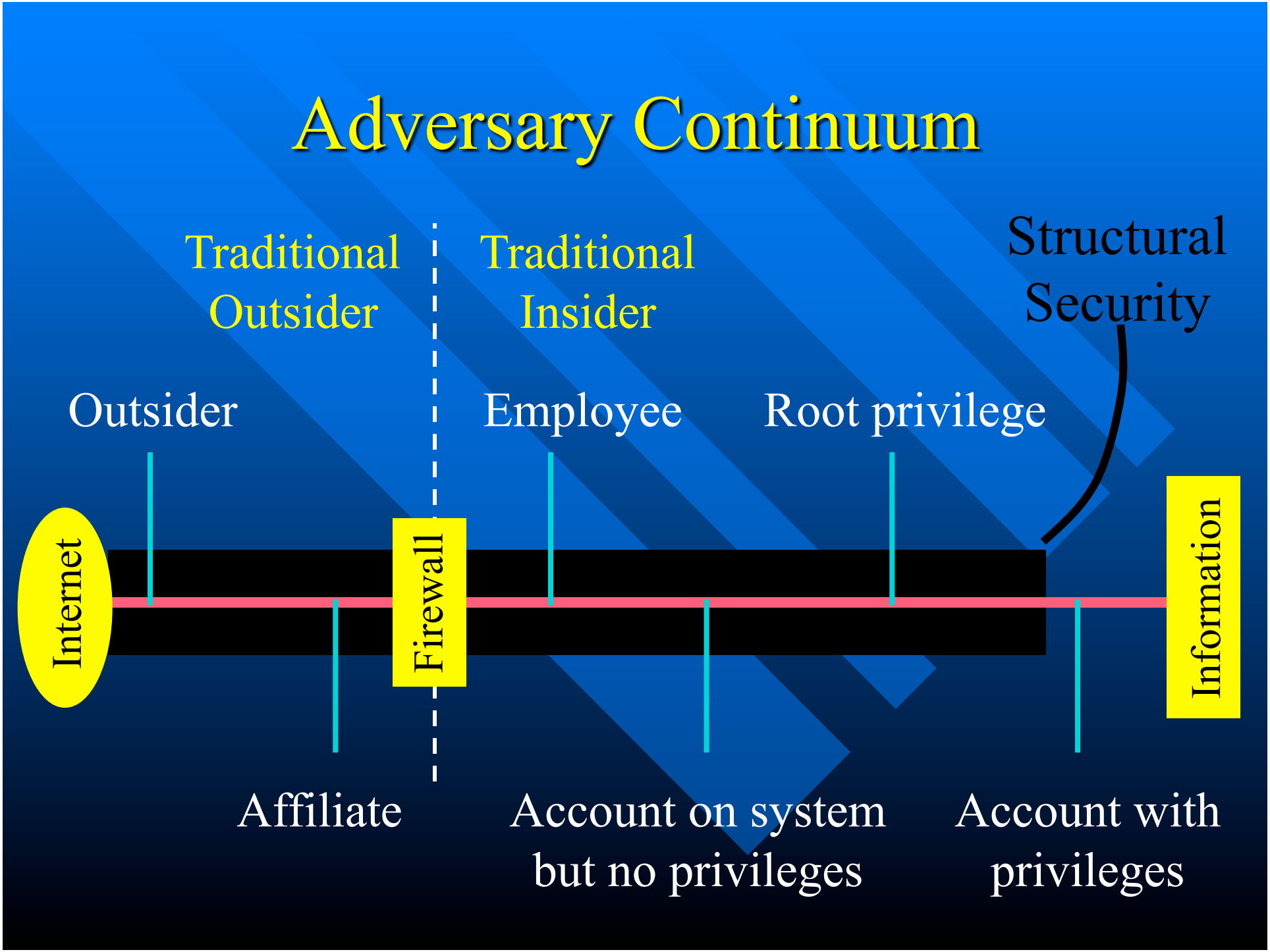
Simple Things Work

- Knuth-Morris-Pratt
  - Compute Prefix: 10 lines of code
  - Perform Match: 12 lines of code
  - Still used in ASIM sensors
- Transcripts
  - Still used in ASIM sensors
- Fingerprint for tracking (DIDS)
- Fingerprint of sessions (Network Radar)

Simple Questions Are Not Asked

- Why do signature-based systems generate so many false alarms?
  - Poor quality control?
  - Need more expressive engines?
  - Approach is fundamentally flawed?
- What percentage of systems with encrypted services run host-based IDS systems?
- What percentage of machines are running automatic update features?

Adversaries


Adversary Continuum
Traditional Outsider
Traditional Insider
Structural Security
Outsider
Employee
Root privilege
Internet
Firewall
Information
Affiliate
Account on system but no privileges
Account with privileges

Adversaries, Competitors, and Partners

Adversaries, Competitors, and Partners

INTERNET SECURITY SYSTEMS™

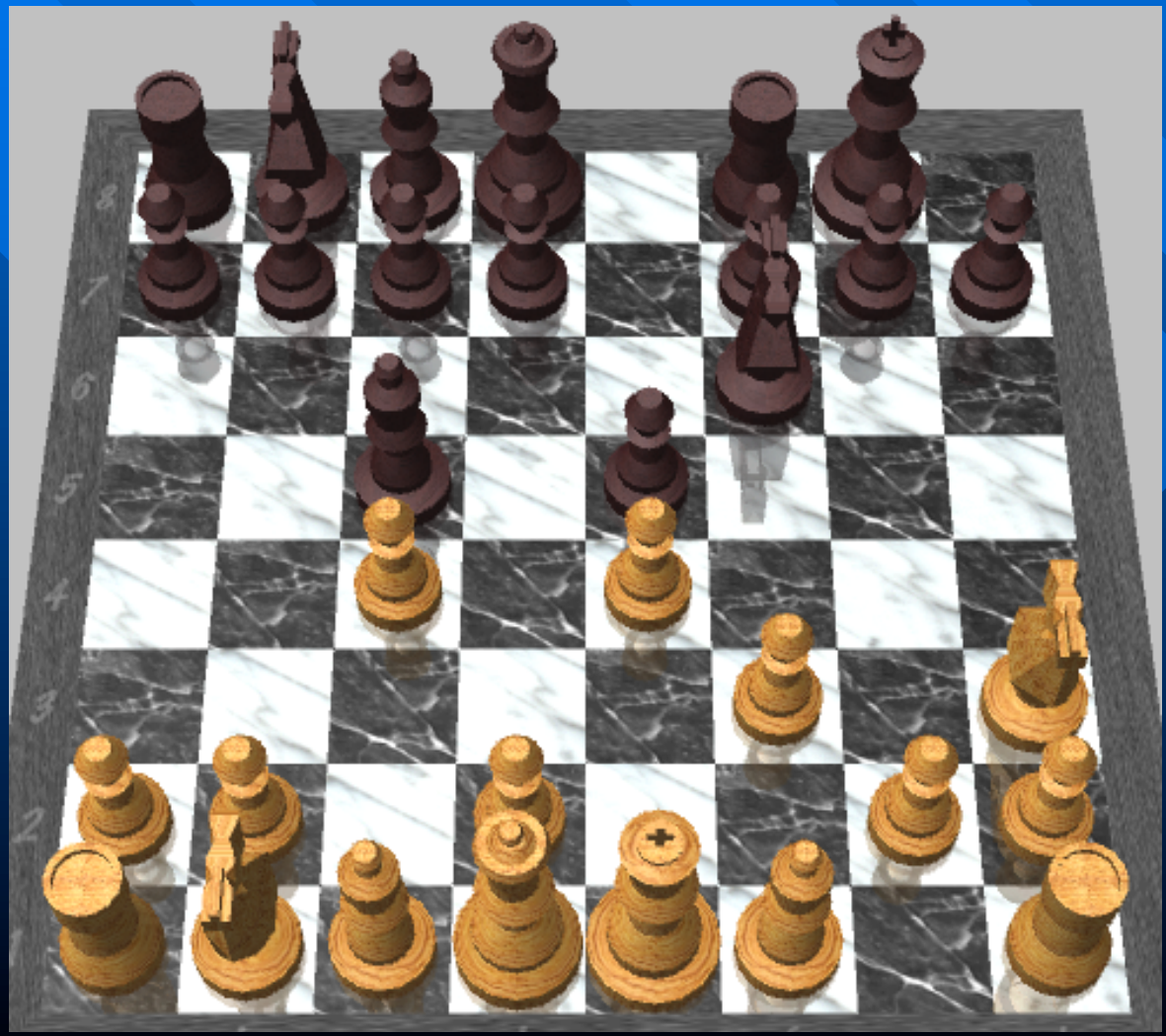
symantec™

Network ASSOCIATES®

SNORT™

Air Force Information Warfare Center
Lackland AFB, Texas

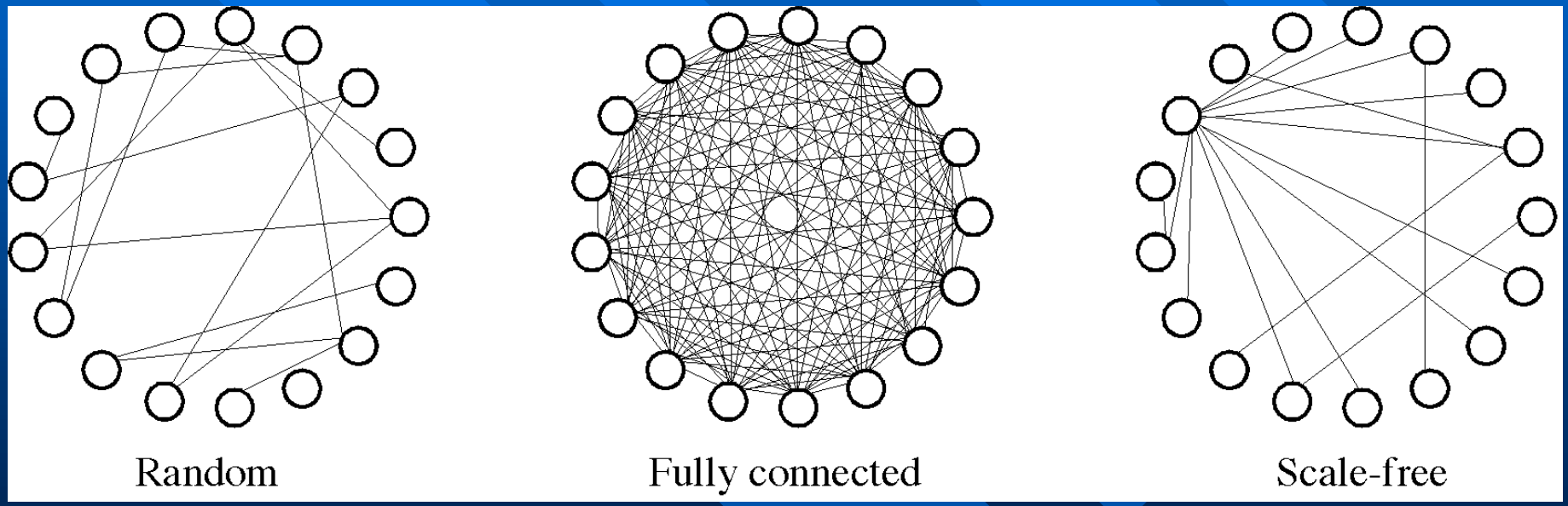
GNU-Chess of MalCode



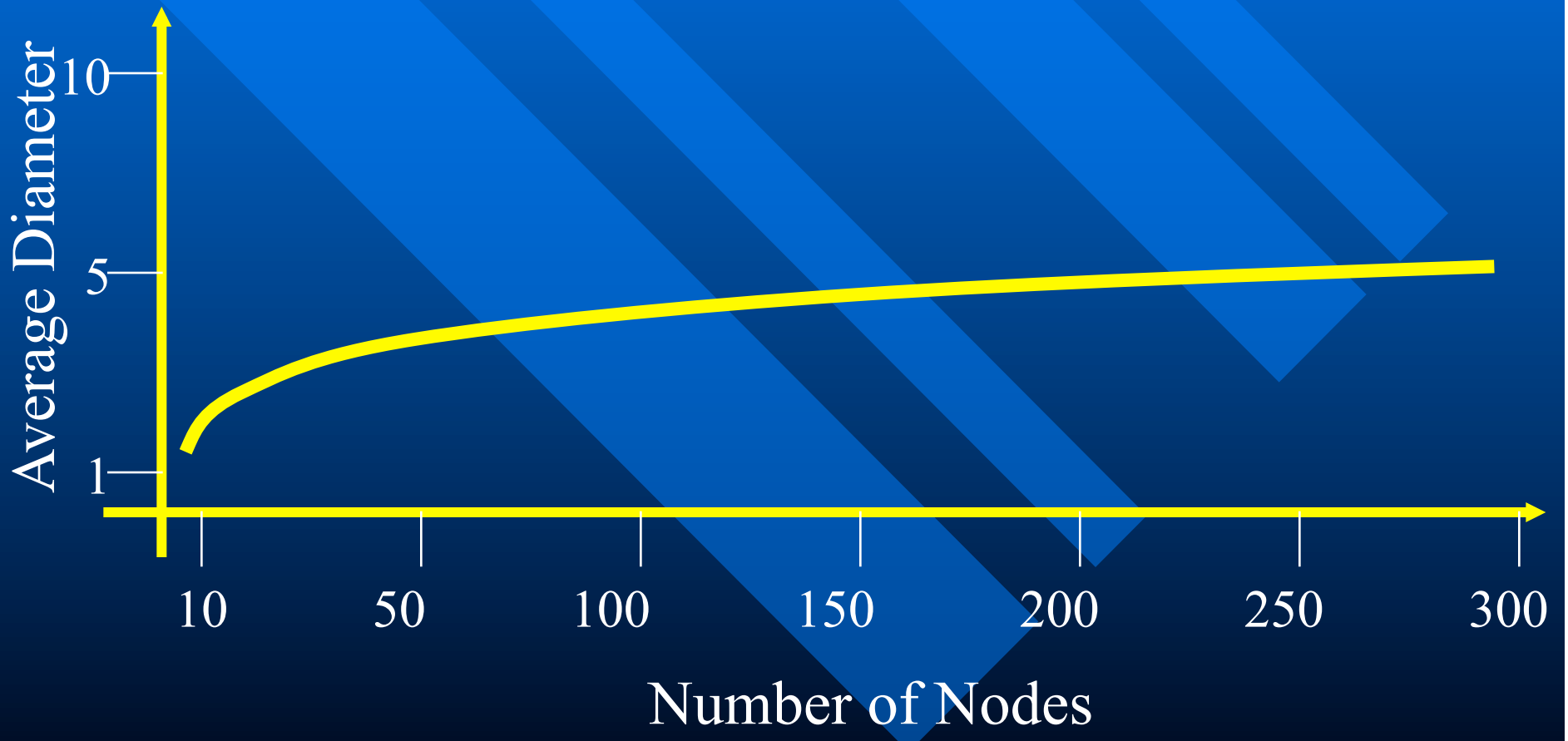
Scale-Free Networks

Overview and Why They Matter

Network Topologies



Meaning of Scale-Free

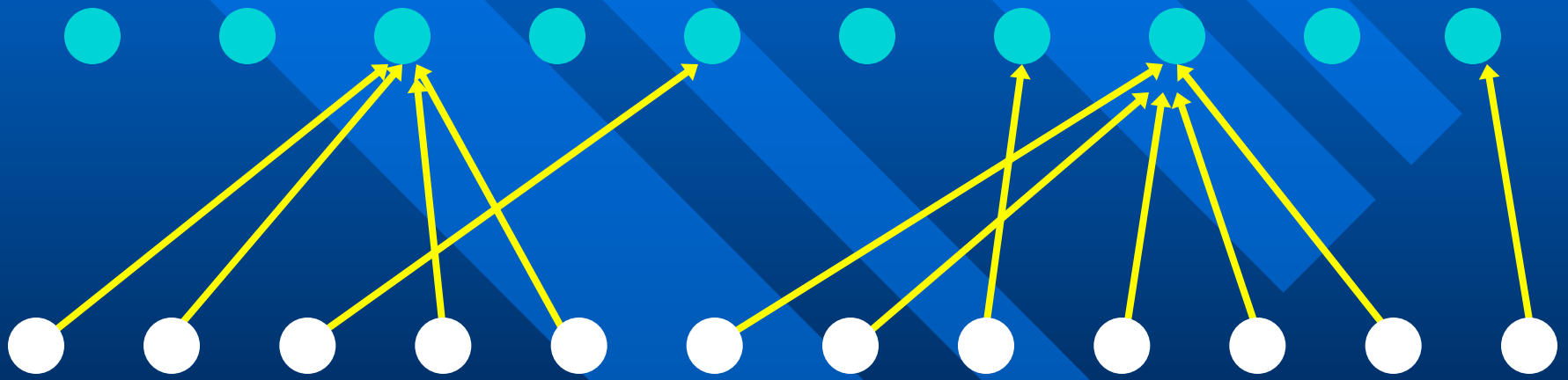


Implications of Scale-Free Networks

- Robust against random attacks/failures
  - If we randomly select and remove a node from the graph, odds are that the node only has a few links to/from it, and the graph hangs together.
- Fragile to targeted attacks
  - If we remove the most highly connected nodes from the graph, the graph quickly falls apart.
- Change your perspectives
  - This fragile aspect can work against us or for us

Vulnerability Network

Known Vulnerabilities



Penetrated Hosts

Implications

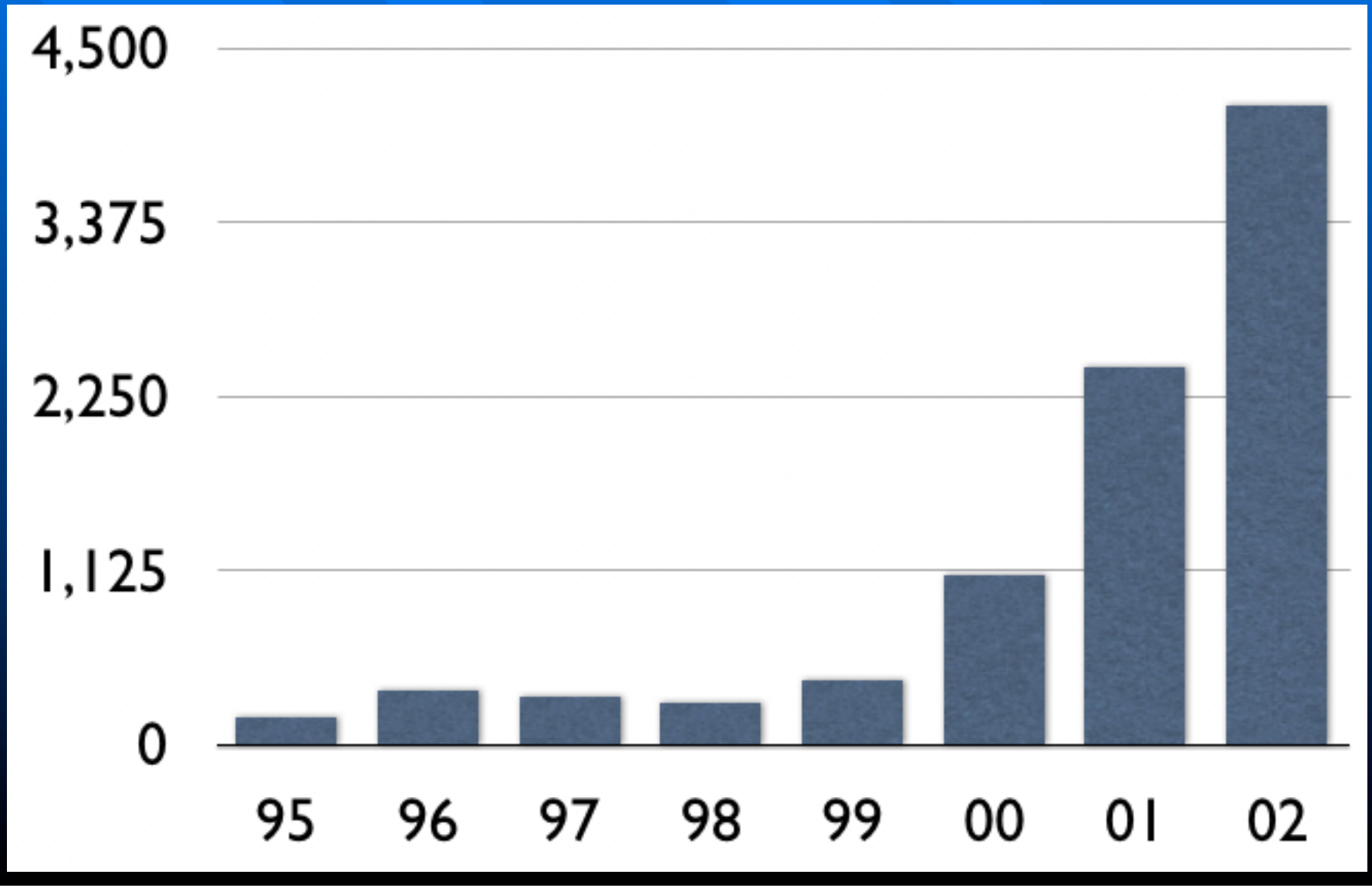
- Random patching of vulnerabilities provides very little actual security
- Targeted patching of super-nodes will provide biggest bang for the buck
- Net-Kuang example
- Bruce Schneier's "Beyond Fear" -- think systems
- Look for Scale-Free networks and determine how they can hurt or help

TrendCenter

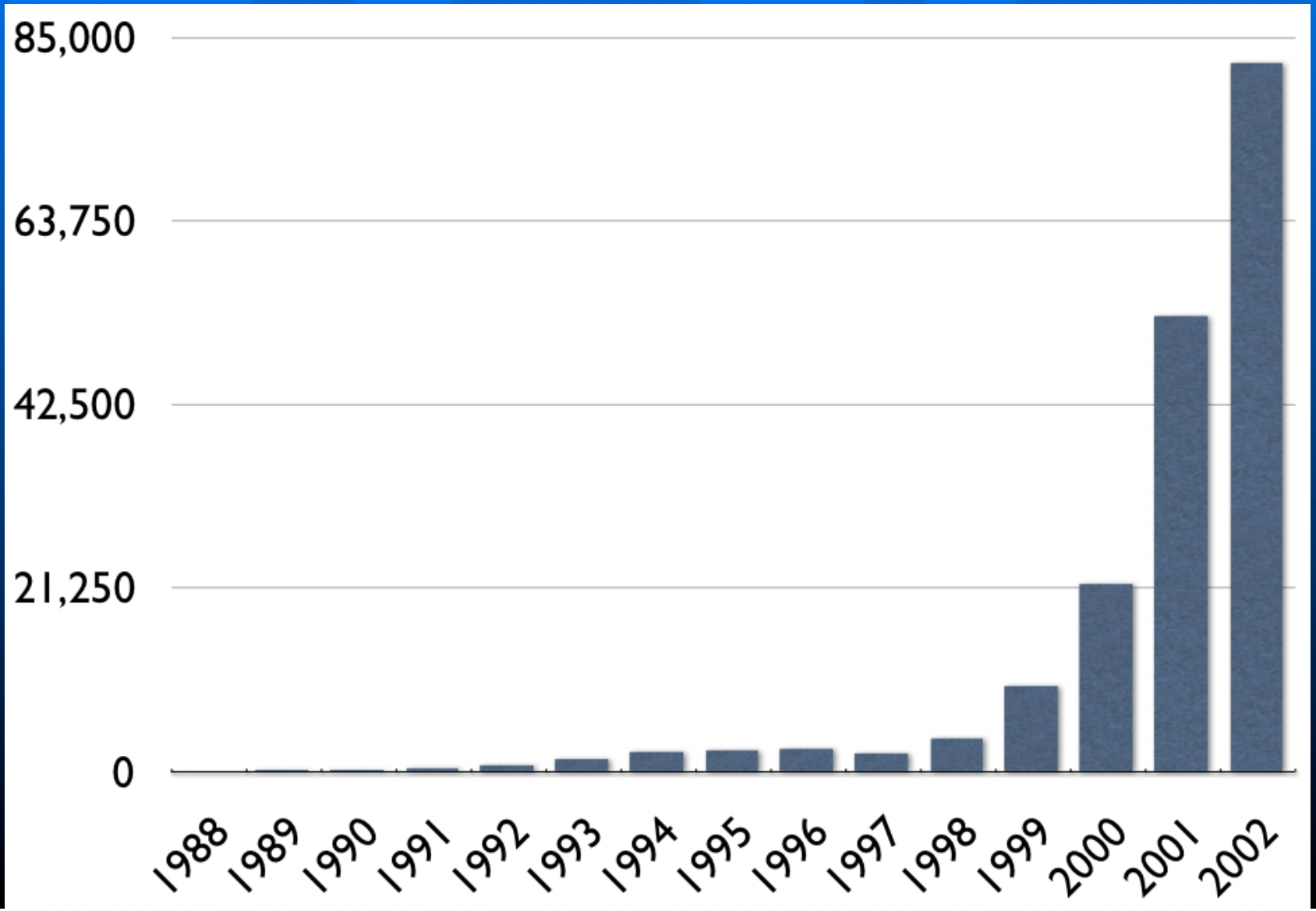
An Early Environment-Aware Effort

Rest In Peace

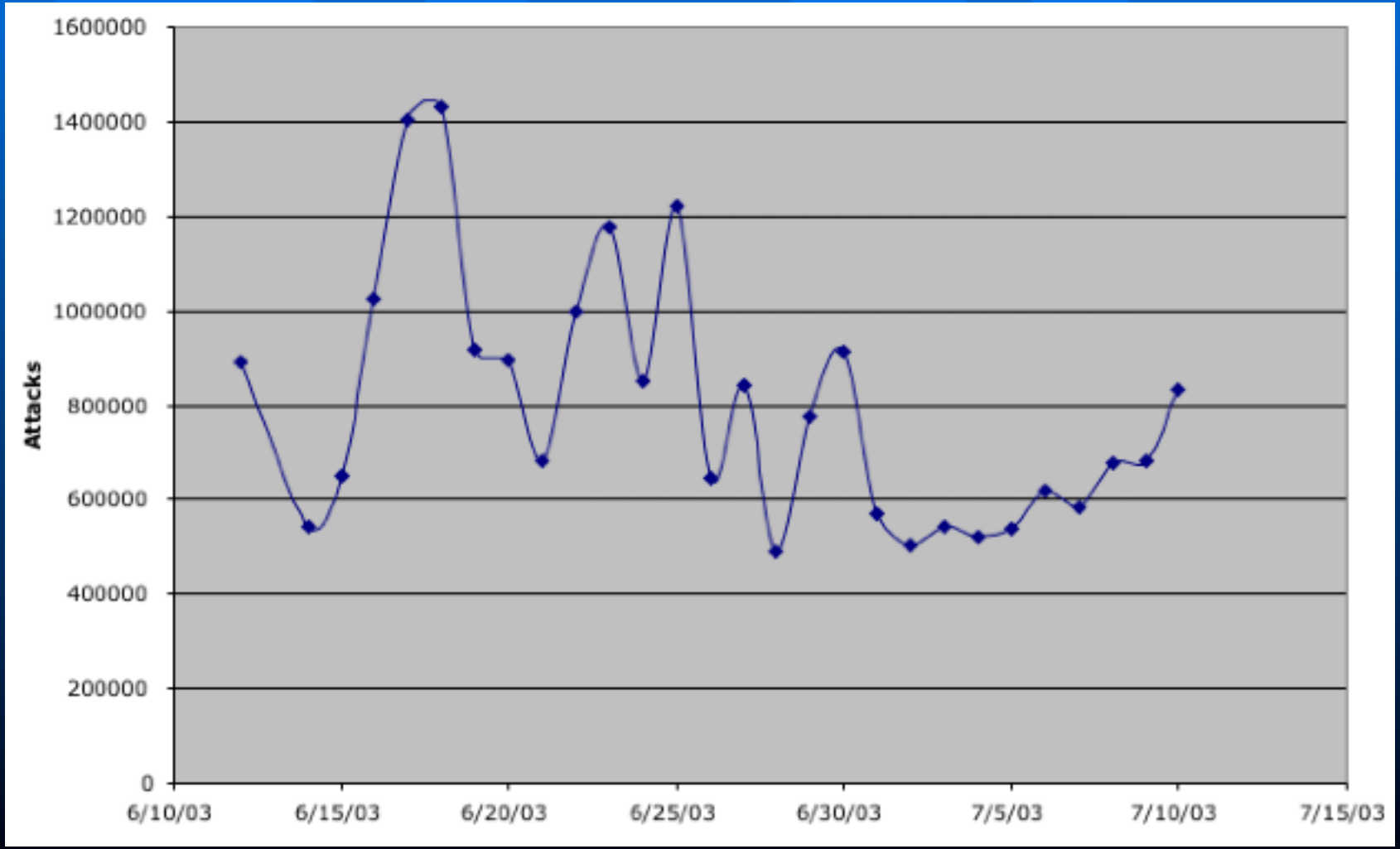
Vulnerabilities Per Year



Incidents Per Year



Reports Per Day at One Site



Counterpane's Event Counter

Featured Items

Counterpane White Paper

Counterpane Presentation

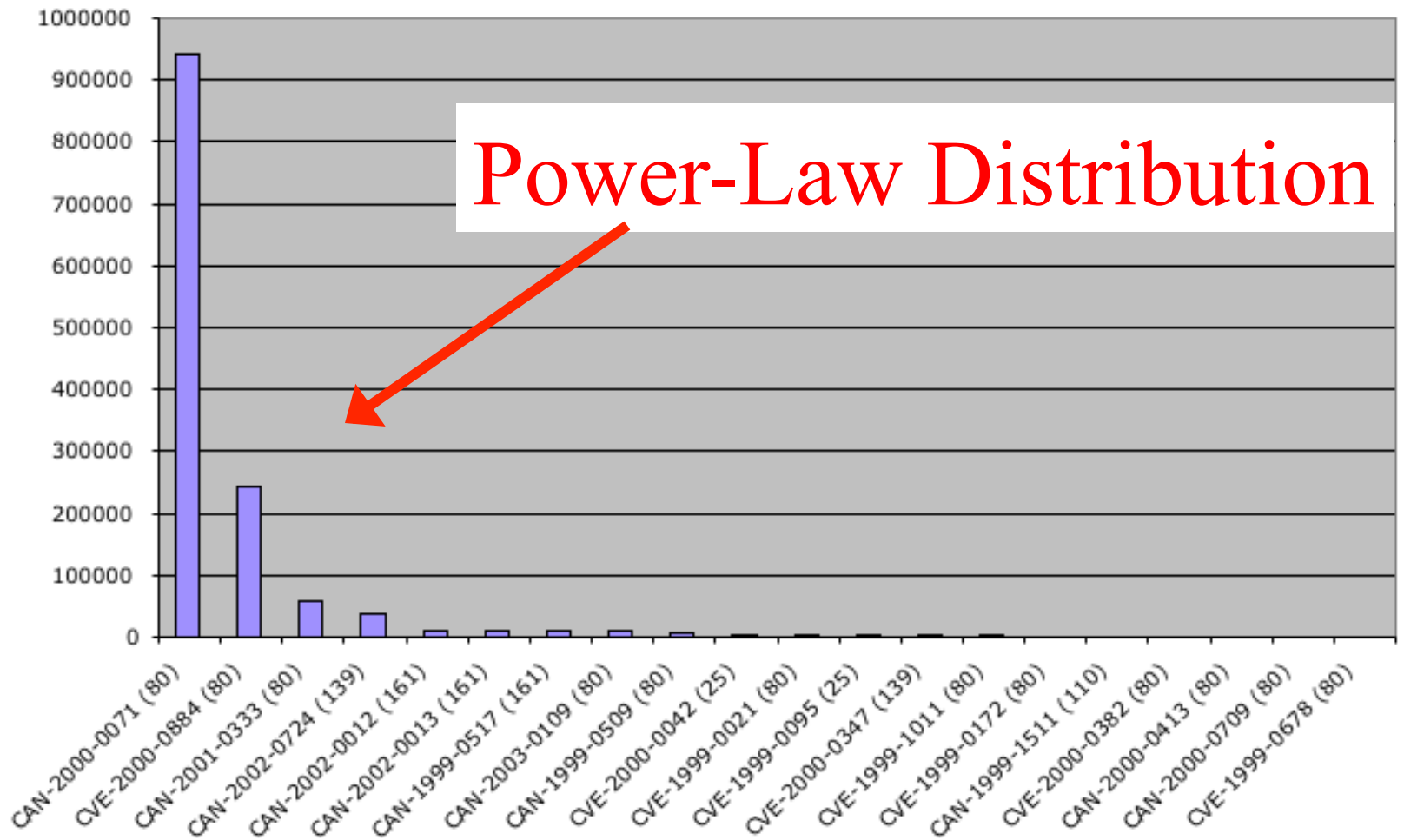
464,309,384,532

Network Events Processed Since 1/1/2003

17,000 Events per Second

ATTACK TRENDS

Analysis | Tools | Contribute | About



Power-Law Distribution

Vulnerability	Port	Score	Details
CAN-2000-0071	80	1000	icat, cve
CVE-2000-0884	80	256	icat, cve

Automatically pulls down latest vulnerability info

Home : Tools

Determines which vulnerabilities you can scan for

Protecting My Network:

Scanner: Nessus

Where: http://www.nessus.org/

Synopsis: Nessus is an open-source vulnerability scanner. Nessus consists of a server, which actually performs the scanning, and a client that sends scanning results

The Perl script below autor
vulnerabilities being activel
vulnerabities your Nessus s
scans a set of target hosts fo

Optional: automatically scan network for those vulnerabilities

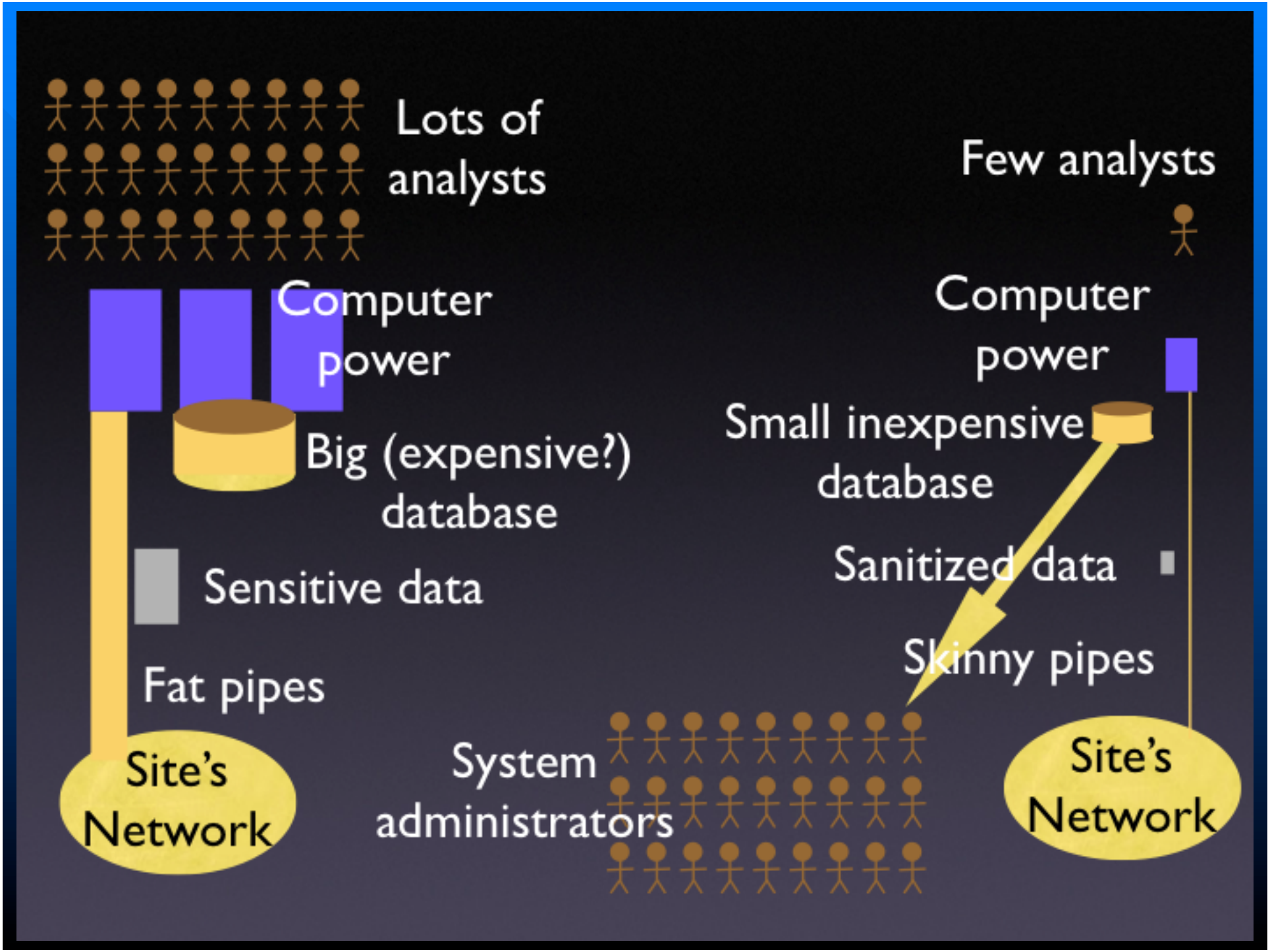
Tool: cverc_v3.pl

Documentation: cverc_v3.txt

Nessus Results

Host List	
Host(s)	**Possible Issue**
169.237.7.105	Security hole(s) found

Vulnerability	netbios-ssn (139/tcp)	. It was possible to log into the remote host using a NULL session. The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and Q246261 (Windows 2000). Note that this won't completely disable null sessions, but will prevent them from connecting to IPC$ Please see http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html . All the smb tests will be done as "/" in domain SIERRANEVADA CVE : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222 BID : 990 Nessus ID : 10394


Lots of analysts
Few analysts
Computer power
Computer power
Small inexpensive database
Big (expensive?) database
Sanitized data
Sensitive data
Skinny pipes
Fat pipes
Site's Network
System administrators
Site's Network

Pipes: How Skinny?

- Original lines: 583,656
  - Sanitized & Summarized: 17,573
  - 3% of original number of “events”
- Original size: ~350 MB
  - Sanitized & Summarized: 630 KB
    - » 0.2% of original size
  - Batch mode compression: 106 KB
    - » 0.03%

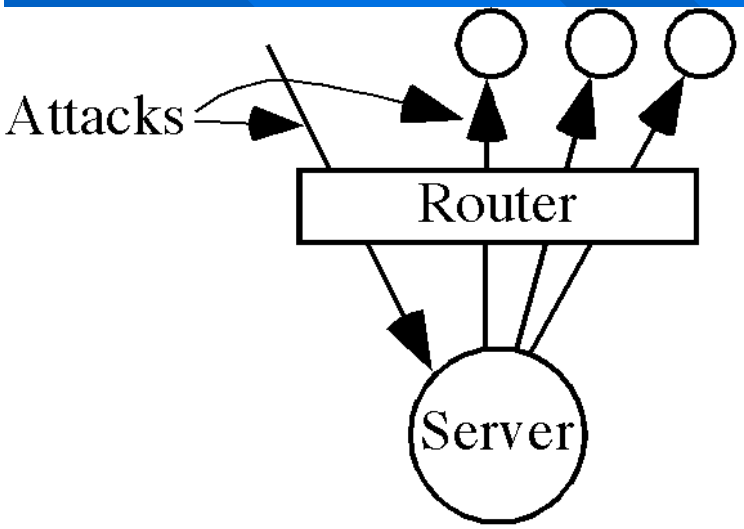
TrendCenter Summary

- Over-the-horizon Intrusion Detection
- Optimizes security per unit of time
  - Predict and Prepare
- Automatically tailor information to a specific site
- Low cost to set up
- No one likes to share data
- New model: Enterprise approach… for now
- Applying efforts to DOE's CPP
- Would the Navy be interested?

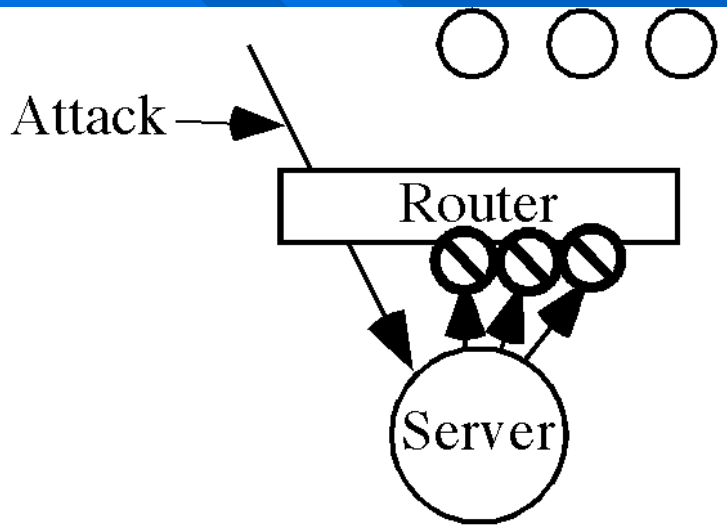
Slightly Richer Analysis

Baby Steps for Firewalls and Servers

Principle of Least Privilege



No Restrictions



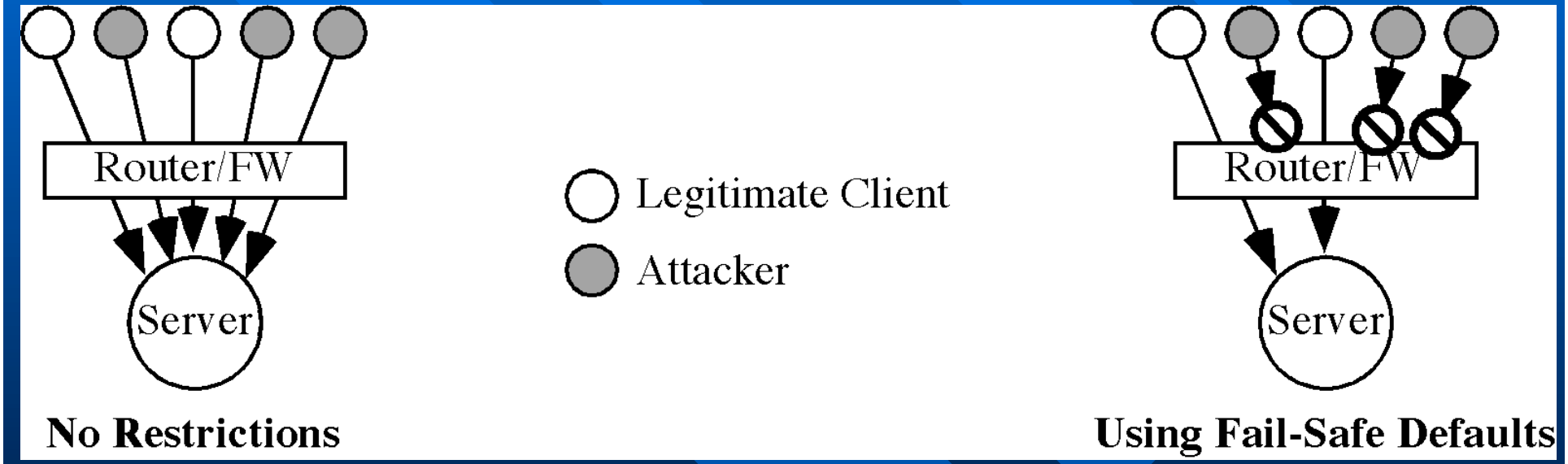
Using Least Privileges

30 Days To Worm Protection

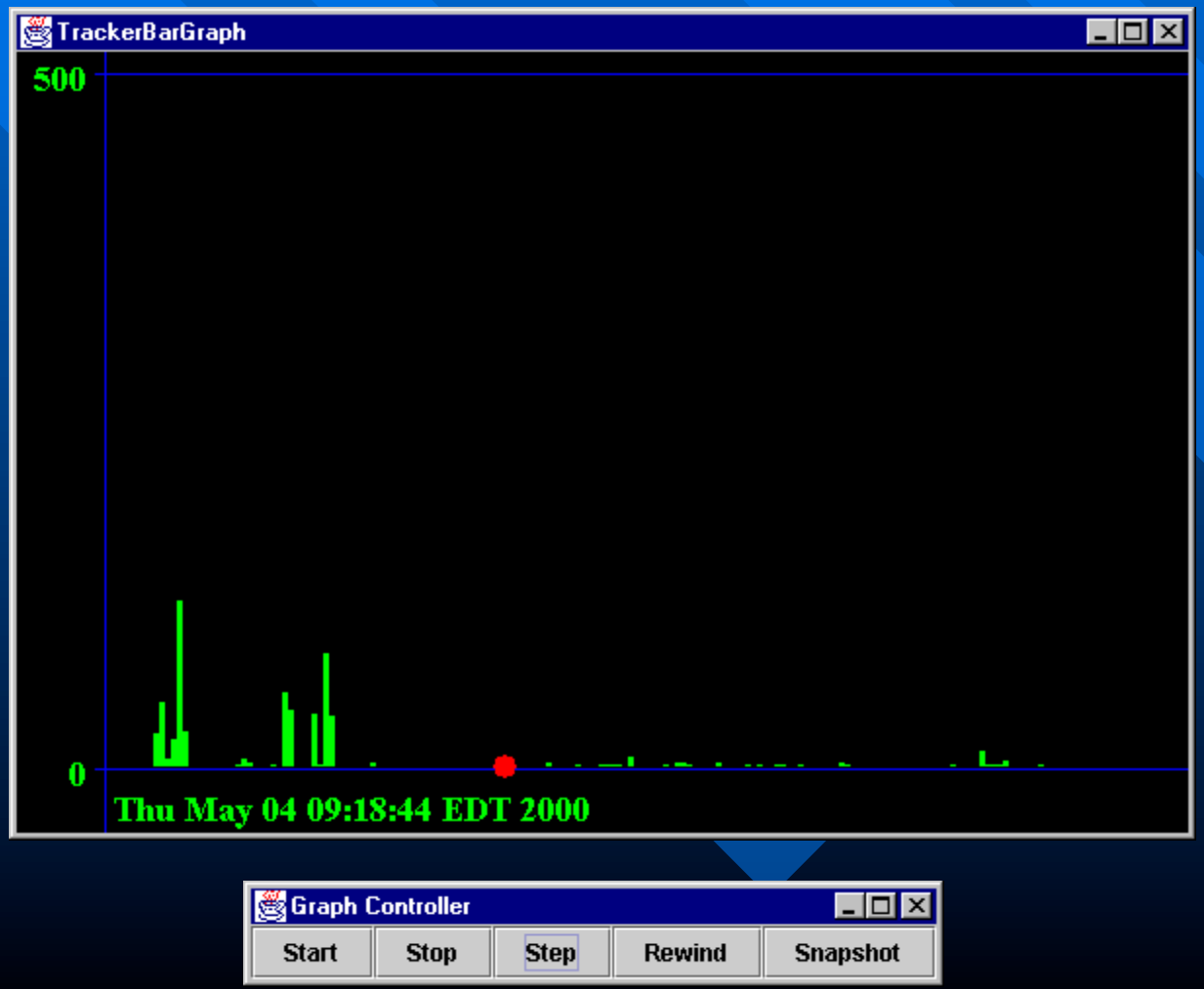
What makes worms different from other attacks is how fast it can spread, and the speed is a product of recruiting successfully attacked systems to contribute to the spread.

Without introducing new hardware or new technology, we can at least retard the speed at which a worm spreads by preventing penetrated systems from launching their own attacks. … This would reduce the spread rate from exponential to something closer to linear.

Principle of Fail-Safe Defaults



Rome: ILOVEYOU Strikes



Rome: ILOVEYOU Strikes

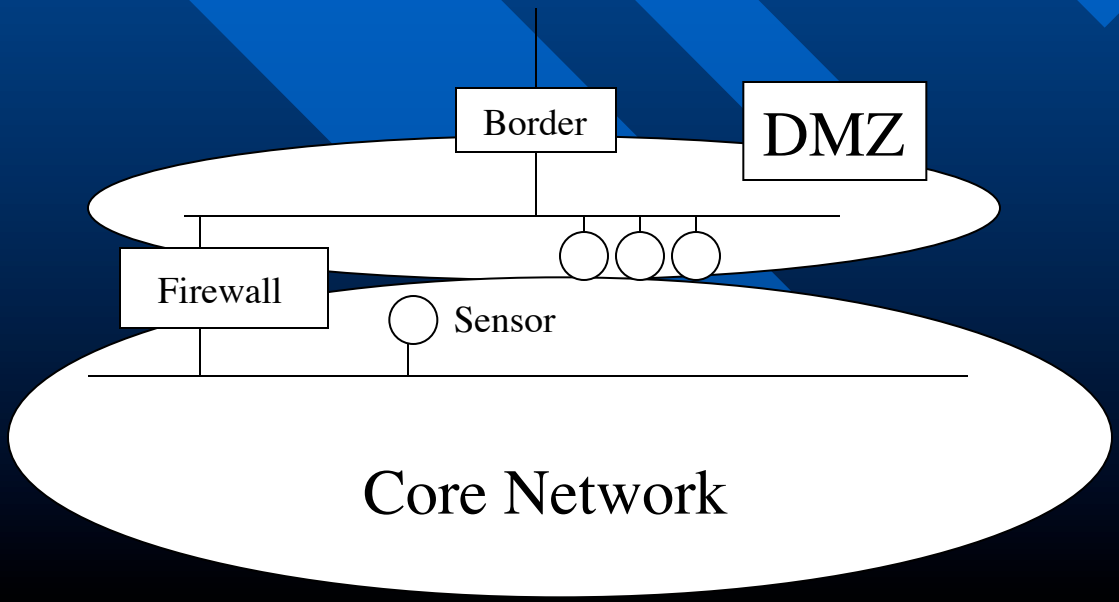
What is this?

Different encoding?

Mass mailing?

Rome Testbed

- Setup
  - 2,010 active IP addresses
  - Border, DMZ, Firewall, Core Network
  - Sensor on Core Network's backbone



Typical Day on the Core Network

- 2,415 inbound paths
  - Path: <client, server, server-port>
- 29 servers accepted inbound connections
- 449 inbound paths were new
  - Excluding one email and one web server
    - » 0 inbound paths were new
    - » 0 anomalous connections
- Conclusions:
  - Rome runs a very tight ship
  - Excluding small number of “public” servers, anomaly detection at network level can work
  - Question: How unique is Rome in this respect?

Configuring Firewalls & Routers

- If Principles of Least Privilege and Fail-Safe Defaults are so great, why aren't people applying these principles?
- Fear of breaking existing capabilities
  - UC Davis example
- Early first steps: Observe and Recommend

iChat AV: Firewalls and NATs

Ports to open for third-party firewalls
A "simple" firewall only allows you to open or close ports, without any additional criteria. If you have one of these, then you should open these ports: 5060, 5190, 5298, 5353, 5678, 16384-16403

If that does not work, try opening all ports in this range: 1024-65535

http://docs.info.apple.com/article.html?artnum=93208

Fears of Security

Security Alert

Patch for a Patch
Microsoft has issued a new patch -- a patch that replaces a previous patch that obviously didn't work for Internet Explorer. To fix the problem, head to Microsoft's website or run Windows Update. It's probably time you did so again anyway.

Apple Pulls Mac OS X 10.2.8 Software Updater

Approved/Edited by arn on Tuesday September 23, 2003 05:37 PM
from the news dept.

For users who have not yet upgraded, the Mac OS X 10.2.8 Update no longer appears in Software Update.

While the majority of users who applied the update have done fine... there are multiple reports of problems -- including users' losing network connections (potential fix) and others are having boot problems on their iMacs/eMacs.

Update: Standalone updaters have now been pulled too.

Security: Just Work Baby

Security will be turned off if the users or administrators perceive that it does or might get in the way of operations.

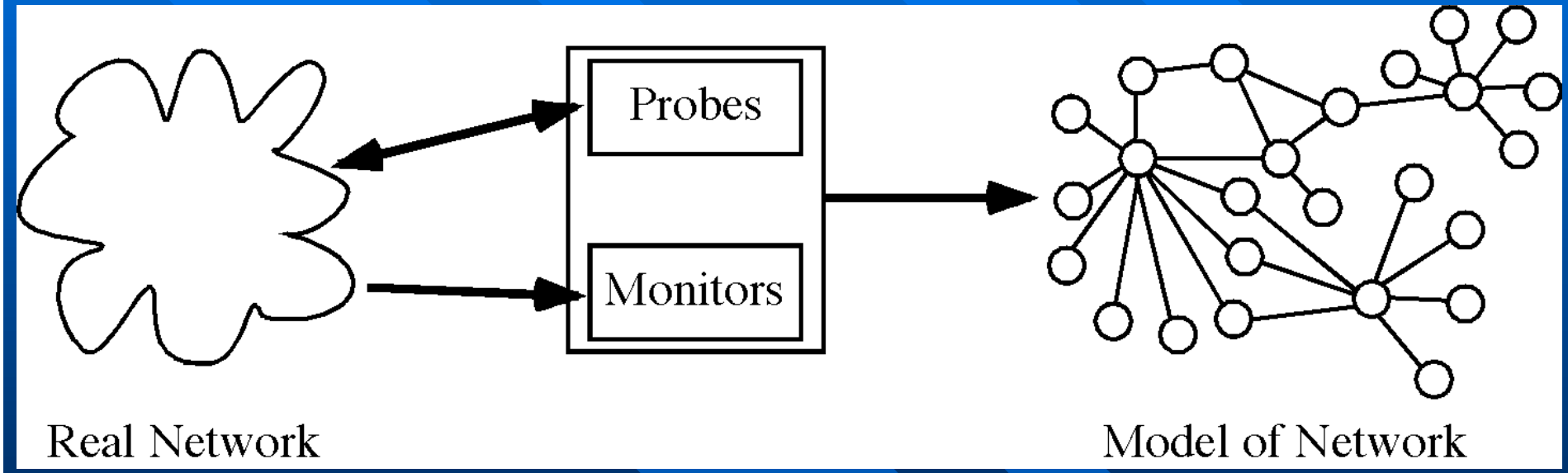
Long-term, our solutions must help in diagnosing why expected operations fails.

Everything that should be allowed to occur can, and everything that shouldn’t occur cannot.

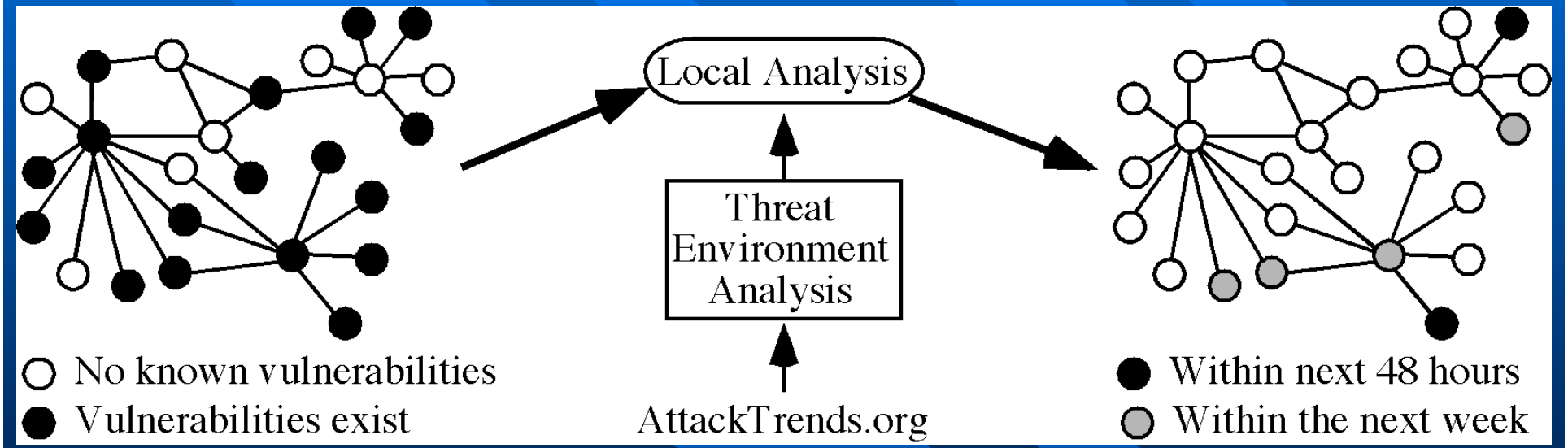
Going Deeper: Modeling the Enterprise

How does the setting of each bit on each host affects every other bit in the rest of the enterprise?

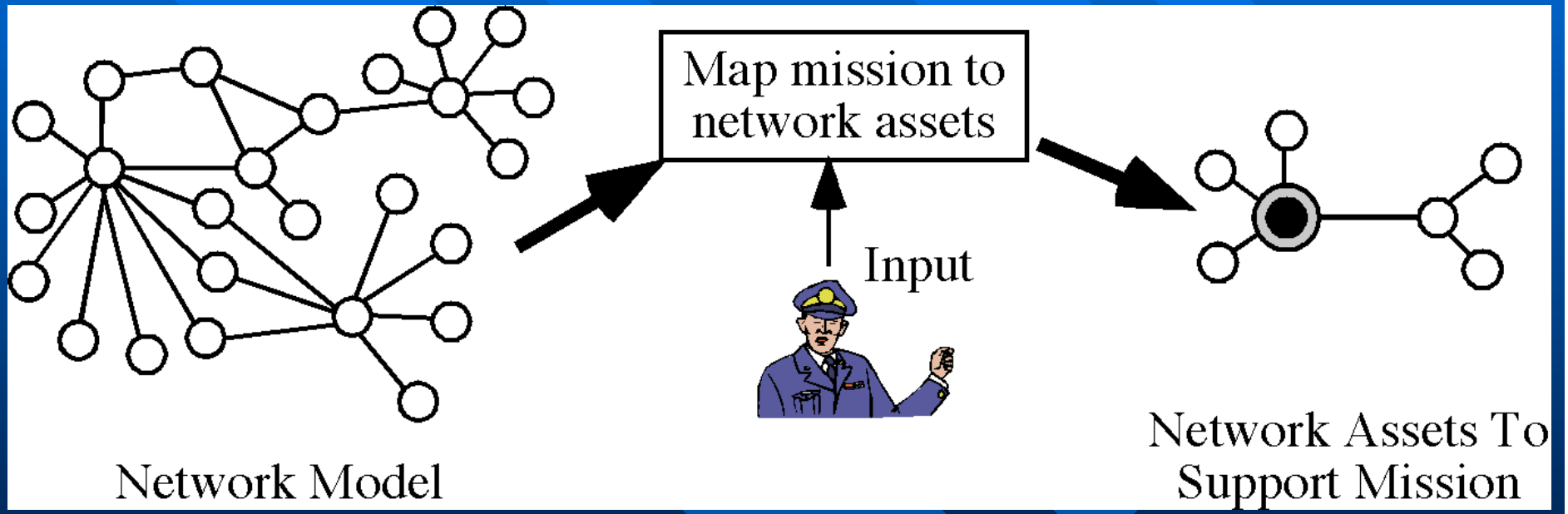
From Network To Model



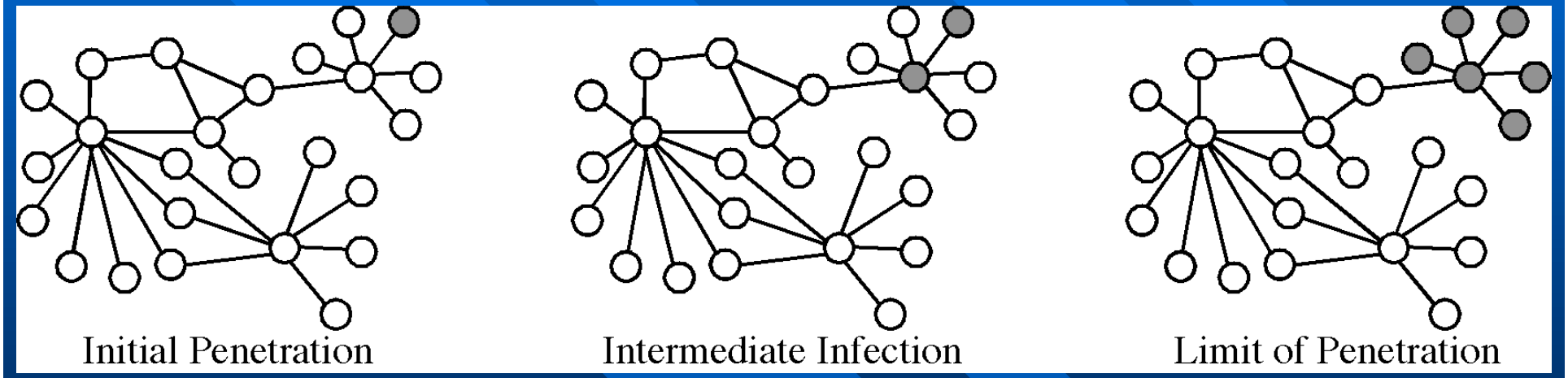
Prioritizing System Patches



Mapping Missions to Assets



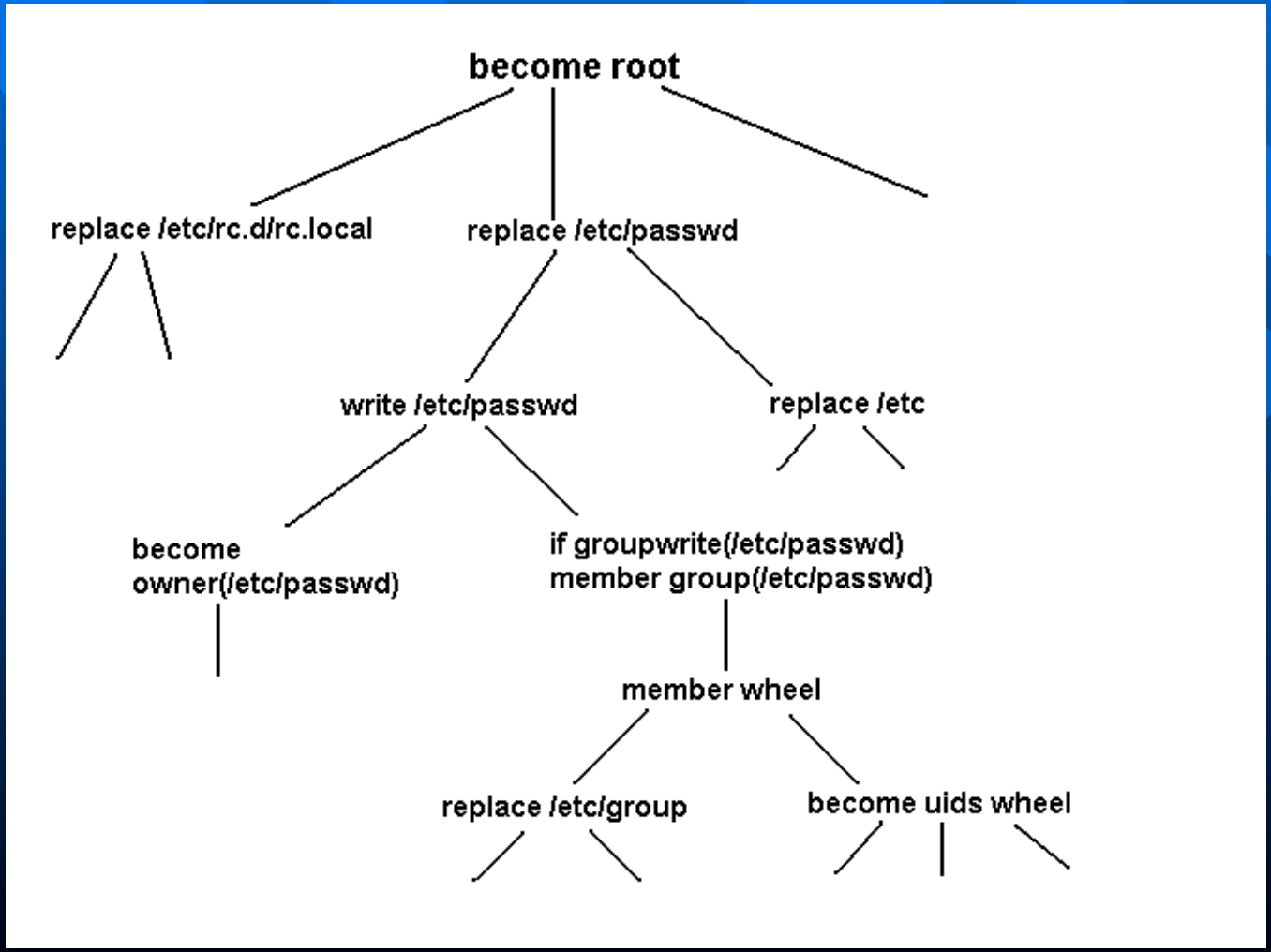
Identifying Cascading Penetration



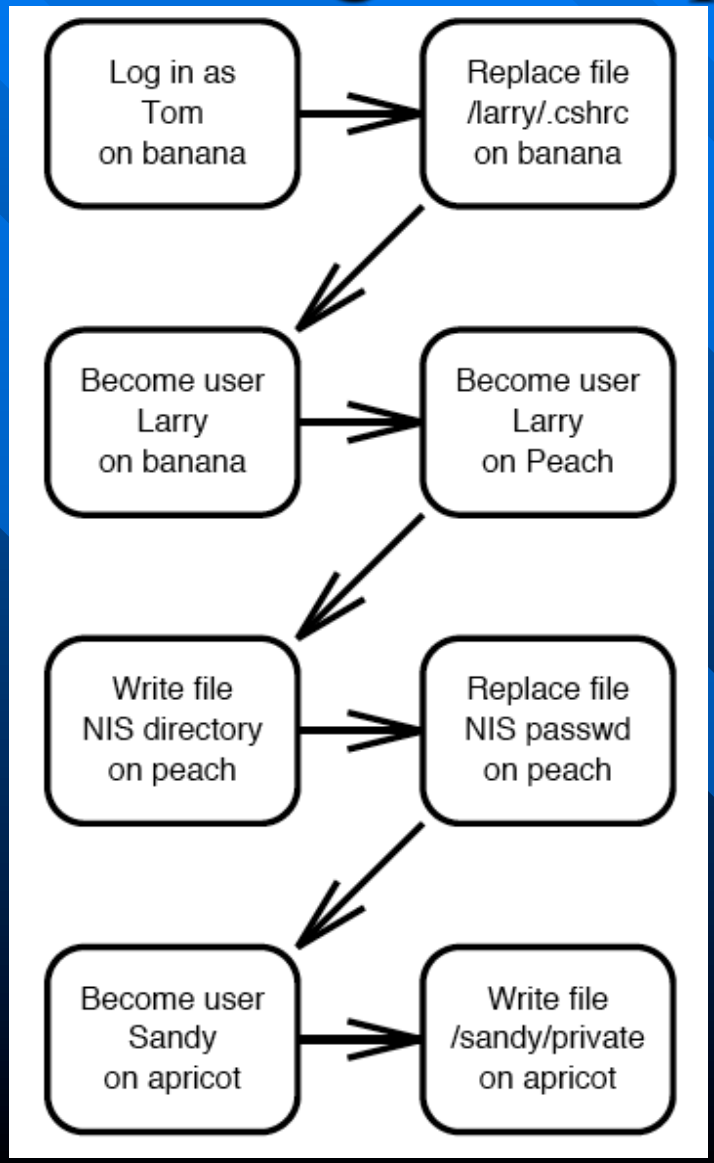
History of Modeling

- Kuang
- Net-Kuang
- LLNL's ACID
- JIGSAW
- CAML
- Many, many others
- Typically described as attack trees or attack graphs

SU-Kuang Example



Net-Kuang Example



JIGSAW Example

Figure 4(b): An Example Concept Specification - RSH Connection Spoofing

```
concept RSH_Connection_Spoofing is

      requires
          Trusted_Partner:    TP;
          Service_Active:     SA;
          PreventPacketSend:  PPS;
          extern SeqNumProbe: SNP;
          ForgedPacketSend:   FPS;
      with
          TP.service is RSH,              #- The service in the trust relation is RSH
          PPS.host is TP.trusted,         #- The blocked host is the trusted partner
          FPS.dst.host is TP.trustor,     #- The spoofed packets are sent to the trustor
          SNP.dst.host is TP.trustor,     #- The probed host is the trustor
          FPS.src is [ND.host,PPS.port]   #- claimed source of forged packets is blocked

          SNP.dst is [SA.host,SA.port]    #- The probed host must be running RSH on the
          SA.port is TCP\RSH,             #-   normal port
          SA.service is RSH,              #-

          SNP.dst is FPS.dest             #- probed host must be where forged packets are sent

          active(FPS) during active(PPS)#- forged packets must be sent while DOS is active
      end;

      provides
          push_channel:       PSC;
          remote_execution:   REX;
      with
          PSC.from    <- FPS.true_src;    #- Capability to move code from attacker to RSH server
          PSC.to      <- FPS.dst;         #-
          PSC.using   <- RSH;             #-

          REX.from    <- FPS.true_src;    #- Capability to execute code on remote host
          REX.to      <- FPS.dst;         #-
          REX.using   <- RSH;             #-
      end;

      action
          true -> report ("RSH Connection Spoofing: TP.hostname")
      end;
end.
```

Summary

- The environment has changed.
  - Detect & Respond is dead
  - Predict & Prepare is current trend
  - General Robustness is the long-term goal
- Long-term adversary: GNU-Chess of malcode
- Scale-free networks
- TrendCenter as an early application
- Early steps: firewalls and servers
  - Security solutions must also help diagnose
- Deep models: ask “what if” questions